<u>AMENDMENTS TO THE CLAIMS</u>

This listing of the claims replaces all prior versions of claims in the application.

<u>Listing of Claims:</u>

1.   (Currently amended) A method for facilitating a secured name space for an
assembly employable by application programs during runtime, comprising the steps of:

        providing a key pair having a public key and a private key;

        providing the assembly with a manifest that contains the public key;

        hashing the assembly;

        encrypting the hash of the assembly with the private key; ~~and~~

        relating the encrypted hash to the assembly; and

        <u>referencing the assembly with a manifest that contains a token of the public key</u>
<u>that is computed by a hash function.</u>

2.   (Canceled)

3.   (Currently amended) The method of claim [[2]] 1, further comprising the step of
determining if the contents of the assembly has been modified by decoding the encrypted
hash value with the public key, determining an actual hash of the contents of the
assembly and comparing the decoded encrypted hash with the actual hash.

4.   (Original) The method of claim 3, further comprising the step of determining if
the publisher of the assembly is the owner of the private key.

2

5.   (Original) The method of claim 4, the step of determining if the publisher of the
assembly is the original owner of the key pair comprising the step of comparing the token
of the public key in the referencing assembly with the public key stored in the manifest of
the assembly.

6.   (Original) The method of claim 1, further comprising the step of determining if
the contents of the assembly has been modified by decoding the encrypted hash value
with the public key, determining an actual hash of the contents of the assembly and
comparing the decoded encrypted hash with the actual hash.

7.   (Original) The method of claim 6, further comprising the step of determining if
the publisher of the assembly is the original owner of the key pair.

8.   (Original) The method of claim 7, the step of determining if the publisher of the
assembly is the original owner of the key pair comprising the step of storing the public
key in a storage medium and comparing the public key in the storage medium with the
public key in the manifest.

9.   (Currently amended) A computer readable medium having at least one computer
executable component employable by an application program at runtime comprising:
        an assembly including a manifest that contains a public key and a hash of the
contents of the assembly encrypted by a private key, the private key and the public key
forming a key pair, the encrypted hash being referenced to the assembly, and a
referencing assembly that references the assembly, the referencing assembly including a
manifest that contains a reduced version of the public key of the assembly.

10.   (Canceled)

11.   (Original) The computer readable medium of claim 9, the assembly being a
dynamically linked library.

3

12.   (Currently amended) A system for facilitating secured name spaces of assemblies employable by application programs at runtime, the system comprising:

a first component adapted to provide a manifest within an assembly with a public key; ~~and~~

a second component adapted to hash the contents of the assembly and encrypt the hash with a private key matching the public key; and

a third component that uses a hash function to compute a token of the public key associated with the manifest, the token is used to reference the assembly.

13.   (Canceled)

14.   (Currently amended) The system of claim [[13]] 12, further comprising a verification component adapted to decode the encrypted hash with the public key and compare the decoded encrypted hash with an actual hash run on the assembly.

15.   (Original) The system of claim 14, the verification component being further adapted to compare the public key in the manifest of the assembly with the token of the public key in the manifest of the referencing assembly.

16.   (Original) The system of claim 12, further comprising a key pair generating component adapted to generate a key pair.

17.   (Original) The system of claim 12, further comprising a binding component adapted to provide binding policy information for determining a version of an assembly that an application program will run if another assembly having the same name resides on the system.

18.   (Original) The system of claim 12, further comprising a verification component adapted to decode the encrypted hash with the public key and compare the decoded encrypted hash with an actual hash run on the assembly.

4

19.   (Currently amended) A system for facilitating a secured name space of an assembly employable by application programs at runtime, the system comprising:

 means for providing a key pair having a public key and a private key;

 means for inserting a public key in a manifest of an assembly;

 means for hashing the assembly;

 means for encrypting the hash of the assembly with the private key; and

 means for relating the encrypted hash to the assembly;

 means for hashing the public key; and

 means for inserting the hash of the public key into a manifest of a referencing assembly that references the assembly.

20.   (Canceled)

21.   (Currently amended) The system of claim [[20]] 19, further comprising means for determining if the assembly has been modified.

22.   (Original) The system of claim 21, the means for determining if the assembly has been modified including means for decoding the encrypted hash with the public key, means for generating an actual hash value and means for comparing the generated hash value with the decoded encrypted hash value.

23.   (Original) The system of claim 22, further comprising means for comparing the token in the referencing assembly with the public key in the assembly.

24.   (Original) The system of claim 19, at least one of the assembly and referencing assembly being a dynamically linked library.

5